International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Sm-Arp: Stochastic Markovian Game Model for Packet Forwarding Based Arp Spoofing Attacks Detection

C. Divya, D Francis Xavier Christopher

Abstract*: *Address Resolution Protocol (ARP) spoofing attacks have become the most pivotal attacks in deteriorating the performance of computer networks. The objective of this paper is to develop SM-ARP, Stochastic Markovian game model based ARP spoofing attack detection scheme.Although many recent techniques have been developed to detect and protect against ARP spoofing attacks, the practical challenges has led to ineffective utilization. The major challenge is that the attackers employing ARP spoofing tend to alter the attack strategy at each point and increases the difficulty in detection and security implementations. The packet forwarding relaying is one suchattack strategy which is harder to detect using traditionally proven methodologies. This paper tackles the packet forwarding relay strategy based ARP spoofing attack strategy by using the proposed SM-ARPto eliminate the attack in a practically feasible manner. The proposed model utilizes a stationary Markov model for optimizing the packet forwarding behaviour of the networks. When an ARP spoofing attack is initiated, the SM-ARP model tracks the changes in the packet forwarding patterns through cache table and detects the misbehaviours. As a security measure, these misbehaved nodes are entitled to recovery and repair process to restore the network to stabilized state. Experiments are conducted to evaluate the performance of SM-ARP in an application for student marks management system. The results prove that the proposed SM-ARP model improves the detection of ARP spoofing attacks with accuracy of 88.2% and also reduces the complexity and errors.

Index Terms*—*Address Resolution Protocol, ARP spoofing detection, cache poisoning, Stochastic Markovian game model, packet forwarding relay strategy, stationary Markov model, students marks management

I. INTRODUCTION

Network security is one of the most pronounced terms in the modern internet days. The rapidly increasing internet usage has led to considerable breaching in security and increased the demand for higher security considerations [16]. The security concerns are the high prioritized issues in the areas of networking, financial services and databases; thus leading to immediate measures for protection against such methods. The management of IP/MAC addresses is vital in the network administration and hence more time and costs are allotted to this process. ARP is mostly utilized for this agreement of hosting the 32-bit IP address translating into the 48-bit MAC address to form temporary IP-MAC pair to minimize the translation time and increase the communication speed [15]. This guarantees the efficient communication and other services in the user networks with higher security. However, the vulnerabilities in the ARP structure have resulted in security breaches by spoofing the IP/MAC addresses. These types of attacks on the ARP are more problematic for the cloud centers and particularly in the open cloud environments [17]. ARP translates the IP address into MAC address by defining the destination through broadcasting and deciding the host through response frames received. When the attacker snoop the IP-MAC address, the attacker forges the ARP response frames and corrupts the ARP cache table [20]. During this chaos, the source network sends the network packets to the wrong MAC address and leads to erroneous communication. The weakness of the ARP was first discovered before four decades and still it is considered as the widely applied attack model for system damage. The major factors that have limited the efficient utilization of protection models are the expensive price of tools and conceived nature of operating systems [25]. The other vital factor is the pattern of modelling the attack strategy. Although many protective techniques have been developed in the recent past to eradicate the ARP attacks, the ARP spoofing attack models and their strategies have evolved to tackle the security models consistently [8].

Recent ARP spoofing attacks are mostly based on new strategies that are undetected through existing detection techniques [7]. The attack initialization through idle hosts from previous sessions and the packet forwarding relay are some of the increasingly utilized strategies in recent times. This paper aims at developing an efficient mechanism to detect and prevent the networks from ARP spoofing attacks initiated through the packet forwarding relay strategies. This is achieved through the Stochastic Markovian game model [11] and is applied to a student marks management application to evaluate its efficiency. The remainder of the article is arranged as: Discussions on recent related works are given in section 2. The proposed SM-ARP model is explained in section 3 while the evaluation results are provided in section 4. Section 5 summarizes this research work and also provides the scope for future researches.

II. RELATED WORKS

Many techniques have been developed in the past decade to detect and protect against the

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
C. Divya , Research Scholar, School of Computer Studies, Rathnavel Subramaniam College of Arts and Science, Coimbatore, Tamilnadu
Dr D Francis Xavier Christopher, Director, School of Computer Studies, Rathnavel Subramaniam College of Arts and Science, Coimbatore, Tamilnadu.

rapidly increasing ARP spoofing attacks. Divya and Christopher [2] developed ARP spoofing protection mechanism using Bayesian Support Vector Regression which models the host configuration and network errors for probability prediction of malicious hosts. This protection mechanism has the ability to use past knowledge for detecting the attacker hosts that were dormant in previous sessions. It also initiates the host recovery process to rectify or replace the malicious hosts for future communication sessions. Moon et al, [4] introduced an ARP spoofing detection model using the routing trace. This model named as RTNSS initiates an agent at the users to detect the abrupt modifications in ARP cache tables and determines the malicious hosts. But, RTNSS has limitations in detecting new pattern of attacks as well as idle attacker from past communication sessions.

Ubaid et al, [6] presented a graph based mechanism to tackle the ARP spoofing attacks. The graph based traversal mechanism detects the location of the forged or compromised hosts through the pattern of the request packets. Once the attackers are identified, the flow rules are installed on the switches to avert the attacker hosts. Xia et al, [9] also introduced an active defense model against ARP spoofing attacks in the SDN OpenFlow networks using the POX controllers. This model utilized an inspector mechanism to detect the suspicious host processors with high accuracy. However, this mechanism is not suitable for complex attacks in volatile networks.Matsufuji et al, [10] proposed a method to detect ARP poisoning using the fitting model of ARP request trend for monitoring the malicious activities. In this method, the destination processors of the ARP request packets are considered for detecting the attackers. However, in this method only the pattern of ARP requests are monitored while the locality and frequency features are not considered.

Song et al, [12] developed DS-ARP scheme for detecting the ARP spoofing attacks based on the routing traces. The attackers are detected through the routing cache table and the protection is initiated using ARP Link Type Control to change the system from dynamic to static. However, even this scheme could not handle the evolving attack strategy patterns.Enciso et al, [13] presented a security model for detecting the ARP attacks and network sniffers through the machine learning supervised classification algorithm. However, this algorithm does have limitations in handling larger data networks.Younes [14] presented a security model for averting the link layer attacks in ARP and Dynamic Host Configuration Protocol (DHCP). This security model functions in the basis of detecting the delays and loss of ARP reply packets for finding the presence of attackers. Then the attacker hosts are avoided for secured communication.

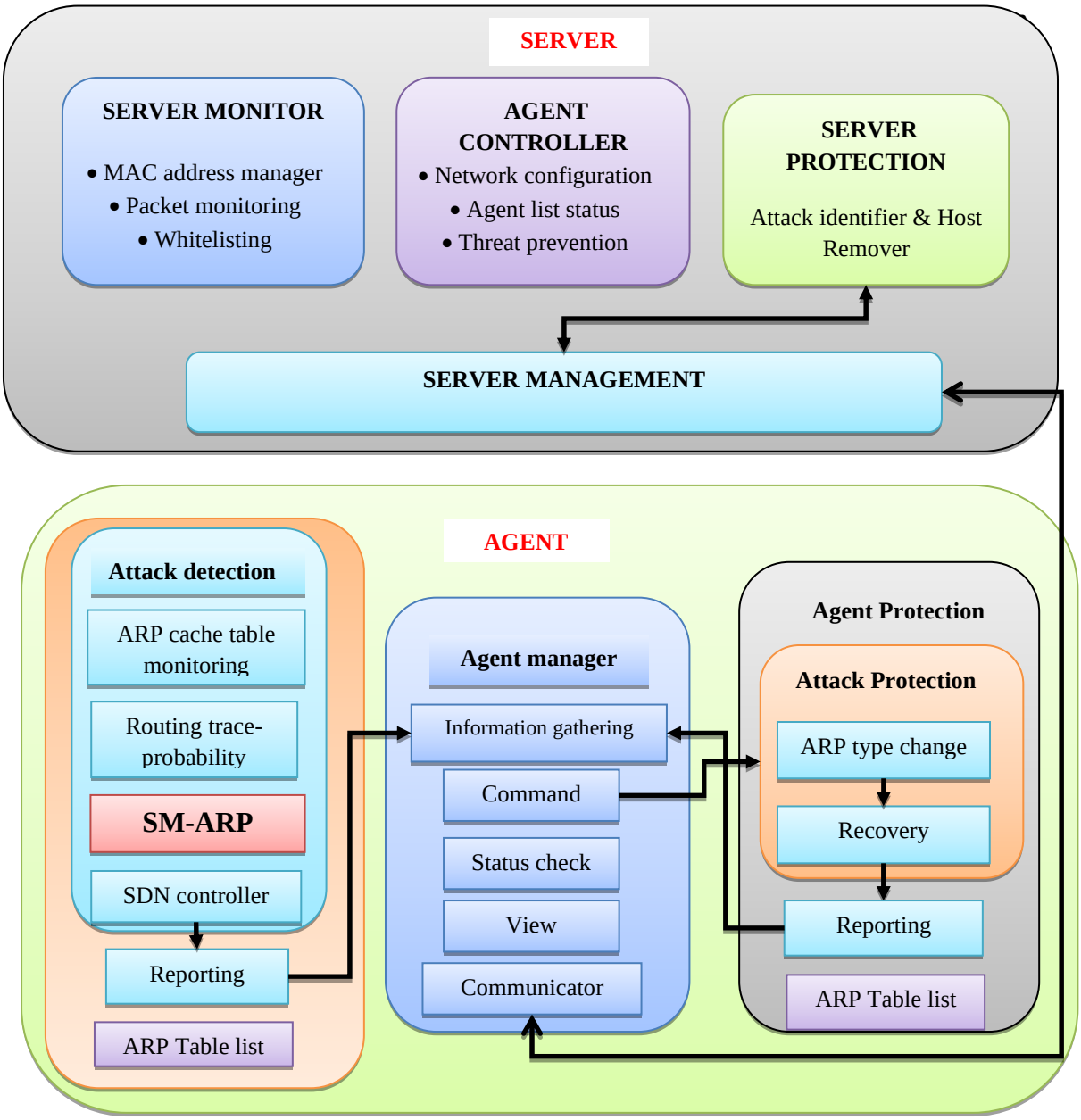
Singh et al, [18] proposed a two-phase scheme for protecting against the ARP attacks. This scheme uses two ICMP probe packets to validate the previous binding hosts and the newly arrived hosts whose validations are combined to obtain the two-phase validation. It also averts the flooding attacks with high accuracy while the only limitation is the complexity of validation. Ullas&Sandeep, [19] proposed a reliable monitoring security system for protecting against the ARP MAC spoofing attacks. This system monitors the frequent network traces and also the cache table to detect the malicious changes and identify the attacker hosts. Nam et al, [21] developed a collaborative approach to protect against the ARP spoofing based Man-in-the-Middle (MITM) attacks. This approach employed the voting fairness model to detect the malicious hosts based on delays and transmission capability.

Sudhakar and Aggarwal, [22] introduced a detection module using ARPWATCH and ARP central server (ACS) to detect the malicious attacks. The ARPWATCH monitors the ARP request packets to each destination and ARP central server (ACS) determines the possibility of attacker host through forged ARP cache table. Kim et al, [23] developed an ARP poisoning attack detection model based on ARP update state of the frequent ARP reply packets. This model outperforms the vulnerabilities of the SDN networks and provides high accurate detection of attackers. Sasan and Salehi, [24] introduced an ARP spoofing detection module for SDN networks using the programmable controllers.

From the literature, it is inferred that the existing AR spoofing detection mechanisms and schemes have limitations in detecting the new pattern of attack strategies. Most specifically, the packet forwarding based strategy of ARP attacks is relatively new and the current protection techniques fail to effectively handle them. This paper obtains the motivation from these related methodologies and builds a new ARP spoofing attack protection model for overcoming this attack strategy.

III. SM-ARP BASED ARP SPOOFING ATTACK DETECTION AND PREVENTION

ARP spoofing attacks are initiated by the attackers through different attack strategy or pattern. When one attack strategy fails to provide the expected outcome, the attacker initiates another pattern of attack. In recent times, many new attack strategies have been introduced by the hackers to infiltrate the networks' MAC address. The packet forwarding based attack strategy is a relatively new procedure in ARP based SDN networks. This attack strategy has many different outcomes like dropping packets, diverting the data, increasing the data rate, corrupting the data, selectively forwarding the data, etc. [3]. It is difficult to detect the action set of the attacker. Stochastic games have been applied for different security problems [5] but it is untested in ARP protocols. Therefore it is aimed to utilize the SM-ARP to tackle this form of ARP spoofing attacks based on the Stochastic Markovian game model. This protection mechanism is modelled based on the Markov stationary game theory for packet forwarding in communication channels.



A) Architecture of SM-ARP scheme

The model consists of a source, a destination and a relay node. The relay node is provided with two buffers to store its own packets and the received packets from source/destination separately. Then the transmission is carried out in either reliable relay or flexible relay based on the current state of the relay. When the relay has attained the complete reliability, it forwards the source packets without considering the state of its own packets through reliable relay. In alternate case of flexible relay, the relay node is provided authorization to decide which packets to forward between its own packets and the received packets from the source. The advantage of using this mechanism is that it differentiates the inferences that caused the loss of packets in such congested traffic scenarios. When the inference is created by the attacker, the data packets can be lost even when the traffic is low. But the intelligent attackers create forged traffic in the channels to avoid being detected by the protection modules. The SM-ARP scheme analyses the physical layer parameters of the lost packets and determines whether the inference is due to legitimate or malicious traffic in an effective manner.

The architecture of the proposed SM-ARP scheme is modelled along the lines of RTNSS [4] and Bayesian Support Vector Regression based ARP protection (BSVR-ARP) schemes [2]. The system is structured on the server agent configuration with the SM-ARP scheme containing two processes: Attack detection process and SDN based attack validation and recovery process. Fig.1 shows the architecture of the SM-ARP scheme. The system architecture is comprised of the server and the agent with separate memory and separate management. The server consists of the monitor, agent controller, protection unit and the complete server management. The MAC addresses of the host are monitored by the monitoring unit along with the packet monitoring and whitelisting. The agent controller is the main component that analyses and tracks the status of each agent host. The network configurations are also described in the agent controller. The protection unit of server analyses the malicious activity

reports and decides on the attacker after which the host recovery or removal is performed. The server management collects information about the hosts, agents and other modules of server and undertakes the functions of communicating; maintaining logs, notification, network management and ARP table validation repository management. The agent is the preliminary working unit of the network and acts as the protection module compared to the authentication property of the server. It includes the attack detection unit, agent management and protection unit. The attack protection and agent management units are similar to that of their counterparts in the server. The attack detection unit performs the process of ARP cache table monitoring, routing trace based probability for detecting previous session attackers, SDN controller and the main SM-ARP scheme. The SM-ARP scheme also incorporates the routing trace based attack verification unit. The detection unit utilizes the stationary Markov model to track and detect the attacks in packet forwarding strategy. The attack detection process is elaborated in the following section along with the attack verification.

B) SM-ARP scheme of ARP Spoofing Attack detection and protection

Game theory based approaches are employed to model any system where two or more players aim to obtain the same goal [1]. Generally, it provides a mathematical analysis to detect the best strategy for each player to achieve the goal. For the proposed SM-ARP, the state of the game is determined by the number of packets in source host and the relay node buffers. The players are the legitimate nodes and malicious nodes by the attackers. The game is modelled as a multi-player game where the fair play rules are enforced by the stationary Markov model. Although this model provides equal opportunity for the genuine host nodes and attacker hosts, the offensive and unfair play results in penalty for the corresponding player in any game. This concept is applied with the loss of packets is termed as offense against the player and the player is deemed attacker. In most cases, the players with the unfair offense is the attacker as it initiates packet drops by forging the original IP-MAC address of the destination. Thus the SM-ARP can detect the attacker and instantly remove them from communication with the help of SDN controller to ensure reliable packet transmission. Fig.2 shows the attack detection process using SM-ARP scheme.

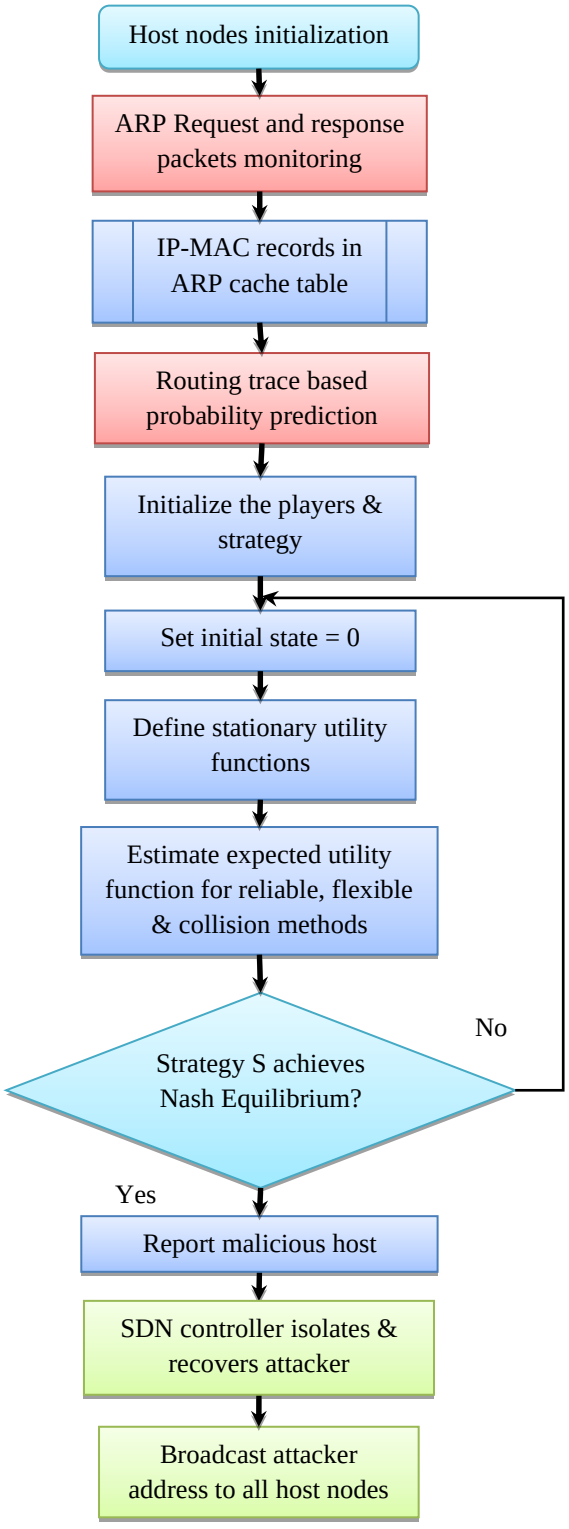


Fig.2. SM-ARP attack detection process

The system model is depicted with the source node, relay node and destination node. The source node has the ability to send packets either directly to the destination or through the relay nodes. The relay node can accept or reject the received packets based on the queue and transmit its own packets as well as the received packets from previous iterations. For simplicity, the two-player game is illustrated in this work by including the source and relay nodes with equal buffer size.

The source node has only single buffer to store the created packets while the relay node has two buffers namely internal buffer to store its own generated packets and forward buffer to store the received packets from the source. The packet generation rates of the source and relay nodes are denoted as and , respectively. At the start of the new session, the buffers are set as empty and the system is modelled as the stationary Markov process. The occupancy state of each buffer is considered as the state of Markov process where in this case there are two possibilities i.e. empty and occupied. This amounts to N^N states equal to 2^3 = states with N number of players.

The game is modelled such that each player knows the current state of the other nodes as well as their possible action sets and outcomes. This leads to a situation where every action of one player can be tackled by the other but the trick lies in the selection of the action which is not known in open. This will also be helpful in averting the attacker more conveniently. When N set of players with Strategy 'S' plays the game, the proposed game model is defined as $(N, \{S_x\}, \{U_x\}), x \in$ where $\{S$ is the strategy of player x with subsets $\{s_x \in S$ and $\{U$ is the x-th player's utility function. Strategy set outlines the behaviour pattern of each player (node) based on which the solution of the proposed game obtains the Nash equilibrium when all players have equal opportunity and best possible strategies. The strategy of x obtains Nash equilibrium S* if

$$\forall_x \in N, \forall_{s_x} \in S_x, \quad U_x(s*_x, s*_{-x}) \geq U_x(s_x, s*_{-}$$

(1)

Where s is the strategy of all players except x. In each stage of the game, the players behave selfishly to obtain their goal and in the proposed model, no player is forced to cooperate with each other. But the fair play is ensured to obtain the attacker details.

The Markov game has $n \times$ state transition matrix denoted by T with n number of states. The elements j in T defines the probability of moving from state i to state j in n+1 time slots. For defining the action sets , the function of current state of the game is denoted as . The next state of the game is obtained by the action set and in the current time slot. For determining the transition probability from to next state q^n, the transition function is generated as $T(q^{n+1}|q^n, A$. Based on this function, the immediate utility of the player x is computed as the function of game action set and current state, expressed as $U_x^n = f(A^n, q$.

In any game, the payoff is the ultimate goal of the players. In the proposed game model, the expected time averaged payoff of player x for any strategy S and initial state function () is computed based on the probability distributions (F) of the game over the action set and states of the game at entire game time. It is expressed as

$$U_x(S, q^0) = \lim \frac{1}{T} EP_{q^0}^S [\sum_{n=1}^T U_x^n(A^n, q^n$$

(2)

Where $EP_{q^0}^S$ is the expectation operation value of F.

The proposed strategy is considered stationary only when the strategy action set depends only on the current state of the game instead of the entire game time. The stationary probability distribution is represented by $\Pi($ with $\Pi(\delta) = \Pi(\delta) \times T($(where $\delta = (\delta_1, \delta_2, \ldots., \delta;$ $T($ is the state transition matrix and represents the matrix multiplication. For k-th state, the stationary utility function of player x is expressed as

$$U_x(\delta) = \sum_{q_k \in Q} \Pi_k(\delta) E[U_x(q_k, \ell$$

(3)

Where $E[U_x(q_k,$ is the expected utility function of player x in k-th state. This equation can achieve Nash equilibrium for the initial state if

$$\forall_x \in N, \forall_{s_x} \in S_x, \quad U_x(q^0, \delta_x^*, \delta_{-x}^*) \geq U_x(q^0, \delta_x, \delta_-^*$$

(4)

This concept when applied to the simplified two-player game model employs either reliable relay or flexible relay methods. The state of the game is illustrated as $\{Q_S, Q_R, Q$ with the elements of this equation denoting the number of packets in the source buffer, relay internal buffer and relay forward buffer, respectively. The mixed strategy of each stationary player in the Markov game model is defined based on the probability distribution of possible action sets. The strategy space of the source node is modelled as (p_{sd}, p_{sr}, p) where p is the likelihood of transmitting a packet from the source to destination directly, p is the likelihood of transmitting packets from source to the relay and $p$is the likelihood of packets waiting at the source. Similarly, for the relay node, the strategy space is modelled as ($p_{rd}, p_f, p_{rw}, p_{ac},$) where p is the likelihood of transmitting a packet from the relay to destination, is the likelihood of forwarding source packets, $p$is the likelihood of packets waiting at the relay, p is the likelihood of accepting source node packets and is the likelihood of rejecting source packets. Based on these mixed strategy functions, the state transition probability is determined.

The expected payoff of the players determines the possibility of the attackers and hence the rewards received will also have significant importance. Each node receives the delivery reward and the relay receives the forwarding reward . The cost incurred for transmission is denoted as C and cost for transmitting a packet from source to relay is . Likewise the cost for transmitting between the nodes is formulated. The delay cost or waiting cost occurring due to attacker collision is and relaying delay cost is . Using the likelihood, cost and reward functions, the utility functions of source and relay nodes can be computed using Eq. (3) and expressed as

$$U_1(\delta) = \Pi_2(\delta) \times \{(R^d)\} + \Pi_4(\delta) \times \{(R^d)\} + \Pi_5(\delta) \times \{p_{sd}(R^d - C_{sd}^t) + p_{sr} \cdot p_{ac}(-R^f - C_{sr}^t - C^r) + p_{sr}(1 - p_{ac})(-C^w - C_{sr}^t) + (1 - p_{sr} - p_{sd})(-C^w)\} + \Pi_6(\delta) \times \{(R^d - C^w)\} + \Pi_7(\delta) \times \{p_{sd}(1 - p_{rd})(R^f - C_{sd}^t) + p_{sd} \cdot p_{rd}(-C^w - C_{sd}^t) + p_{sr}(1 - p_{rd}) \cdot p_{ac}(-R^d - C_{sr}^t - C^w) + p_{sr}(1 - p_{ac} + p_{rd} \cdot p_{ac})(-C^w - C_{sr}^t) + (1 - p_{sr} - p_{sd})(-C^w)\} + \Pi_8(\delta) \times \{(R^d - C^w)\}$$

(5)

$$U_2(\delta) = \Pi_2(\delta) \times \{(-C_{rd}^t)\} + \Pi_3(\delta) \times \{p_{rd}(R^a - C_{rd}^t) + (1 - p_{rd})(-C^w)\} + \Pi_4(\delta) \times \{(-C_{rd}^t - C^w)\} + \Pi_5(\delta) \times \{p_{sr} \cdot p_{ac}(R^f)\} + \Pi_6(\delta) \times \{(-C_{rd}^t)\} + \Pi_7(\delta) \times \{p_{rd}(1 - p_{sr} - p_{sd})(R^d - C_{rd}^t) + p_{rd}(p_{sr} + p_{sd})(-C^w - C_{rd}^t) + (1 - p_{rd}).p_{sr} \cdot p_{ac}(R^f - C^w) + (1 - p_{rd})(1 - p_{sr} \cdot p_{ac})(-C^w)\} + \Pi_8(\delta) \times \{(C_{rd}^t - C^w)\}$$

(6)

Adding the likelihood of forwarding source packets, , to the Eq. (5) and (6) provides utility functions for the flexible relay method. Thus obtained utility functions are also similar to the reliable relay method.

In a similar approach, the probability of bit error (p will alter the overall packet failure or drop probability. The probability for loss of source and relay nodes' packets can be formulated as

$$p_e(s|d) = p(\bar{s}, r|d) + p(\bar{s}, \bar{r}|$$

(7)

$$p_e(r|d) = p(s, \bar{r}|d) + p(\bar{s}, \bar{r}|$$

(8)

Where $p(s, r|$, $p(\bar{s}, r|$, $p(s, \bar{r}|$ and $p(\bar{s}, \bar{r}|$ are the likelihoods of successful reception of both packets, relay packets only, source packets only and failure of both packets, respectively during the attacker collision process leading to unfair or malicious entry. Applying these probabilities to Eq. (5) and (6) provides the utility functions for adaptive method followed during collision in which both the reliable relay and flexible relay methods are performed adaptively. Thus the malicious nodes in packet forwarding process can be effectively detected and the SDN controller verifies the attacker presence. Algorithm 1 summarizes the proposed ARP spoofing detection process of SM-ARP.

Algorithm.1: SM-ARP for ARP Spoofing Attack detection

Input: Node i that send ARP frame
Begin
Initialize n host nodes
ARP Request frame & Response packets processes
Add Routing trace
Initialize players and game strategy
Assume Nash Equilibrium
Set $State \leftarrow$
For each player i
  Define utility functions
  Estimate expected utility functions using Eq. (5) to (8)
    If Strategy $S \approx Nash\ Equilibriu$
      Flag and Isolate i
      Update ARP cache table
    Else
      $State \leftarrow State + 1$
    End if
  Until termination conditions met
  Return Attacker list
End for
End

IV. EXPERIMENTS AND RESULTS

The proposed SM-ARP scheme is evaluated in a prototype simulation model developed in MATLAB (v.2013a). This simulation model is set up similar to that of the BSVR-ARP with the addition of a student mark management application demonstration to elaborate the working application of SM-ARP. It can be extended to any similar application involving ARP and SDN. The experimental environment for SM-ARP scheme is given in Table 1. The initial setup is provided with 100 hosts and it can be flexibly increased or decreased as per the need of the application.

TABLE 1
SIMULATION ENVIRONMENT

OS	Windows 8, 32bit
Processor	Intel core i5 3470 3.2 GHz
RAM	4GB DDR3
Storage	500GB Intel SSD SC2CT060A3 ATA device
Network bandwidth	1 Gbps
Simulation tool	MATLAB v.2013a
Simulation time	120 seconds
Network area	1000x1000 m
Packet size	80 bytes
Application	Student Marks Management
Maximum Students	100

A) Student Marks Management system

The proposed student marks management system comprises of layout for the inclusion of student marks for pre-defined number of subjects. The maximum number of students is set as 100 since the complexity of the system increases above 100. The number and name of subjects is user defined and hence the system can be applied to any course. Similar entry based applications can also be employed in this model. The proposed application is tested under two cases: without attacker and with the presence of attacker hosts. Fig.3 shows the input phase of the application where the name and mark details for three subjects are needed to be entered. In this evaluation, the selective packet dropping behaviour of the attackers is modelled for illustration.

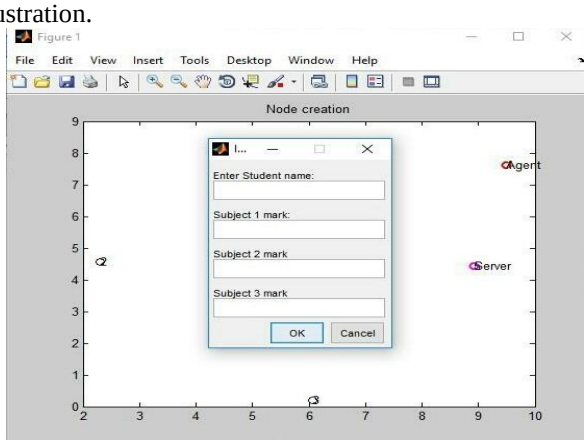


Fig.3. Student Marks Management System Input stage

The received data in the two cases are illustrated Fig.4. Fig.4a) shows the output phase of the application when there is no attacker or malicious hosts. In this case, the students' marks entered are displayed as provided in the input stage (shown in [ ] brackets).

The normal transmission phase does not require the utilization of SM-ARP and hence it stays in background without increasing the cost and resource utilization.

```
Node0is attackerNo attack is detected
Information for students
    'Student 1'    [45]    [40]    [48]
    'Student 2'    [55]    [52]    [66]
    'Student 3'    [68]    [75]    [59]
    'Student 4'    [81]    [75]    [70]
    'Student 5'    [84]    [80]    [87]
```

Fig.4a). Normal transmission case (No attacker)

Fig.4b) shows the abnormal transmission case where the packets are lost due to the presence of attacker hosts. In the second case, when there is one or more attacker hosts, the data packets are selectively lost. The attacker hosts in the transmission channels track down the IP-MAC address of the destination during the packet forwarding process. In this case, the attacker drops the data packets containing the students' marks and the outcomes displays only the students' names while the marks entered in input stage are lost.

```
MAC Address
Attacker
E8-ED-E6-CF-D8-EE
USer
F1-C8-CF-D2-D2-E6
Information of students
    'Student 1'
    'Student 2'
    'Student 3'
    'Student 4'
    'Student 5'
```

Fig.4b). Abnormal transmission case (Attacker detected)

When the packets are lost, the SM-ARP through the game theory model detects the collision location and tracks the malicious host which was responsible for the packet loss. The suspected host is flagged and removed from the communication channel. Then the original IP-MAC address of the suspected host is retrieved from past sessions stored at log files of server management and compared to verify the attacker. This host is then isolated and undergoes the recovery/removal process to stabilize the network. Thus the SM-ARP scheme effectively detects and protects against the ARP spoofing attacks in the proposed marks management system.

B) Performance evaluation

The performance of the proposed SM-ARP scheme is evaluated and compared with the existing schemes of KNN, SVM, Naïve Bayes, RTNSS and BSVR-ARP. It must be noted that the proposed SM-ARP model also incorporates the routing trace based probability prediction as in BSVR-ARP to eradicate the idle-to-be-turned attackers from previous communication sessions. Comparison of these schemes is performed in terms of detection time, attack accuracy, detection error, false detection probability and packet drop rate.

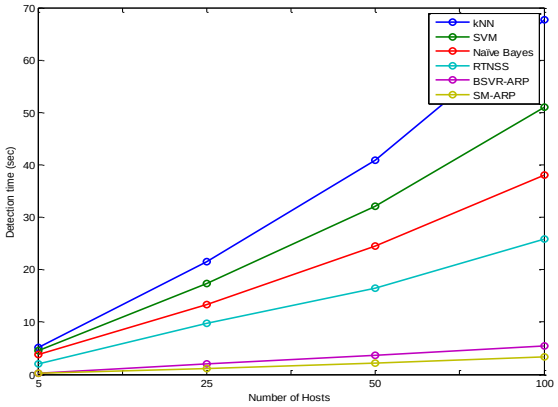


Fig.5. Detection time

Fig.5 shows the comparison of the ARP protection schemes in terms of detection time in seconds. The time taken by the proposed SM-ARP scheme is very less than the other compared schemes. For instance, when 100 nodes are considered for the best schemes, the detection time of SM-ARP is 65% less than RTNSS and 5% less than the BSVR-ARP scheme. The integration of the attack verification process with the detection process of SM-ARP has led to the reduced time.

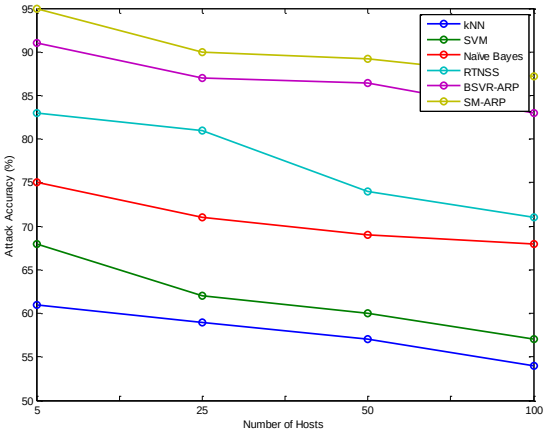


Fig.6. Attack Detection Accuracy

Fig.6 shows the comparison of the ARP protection schemes based on the attack detection accuracy (%). When the attackers are initiated at each case of host nodes, the accuracy of SM-ARP outperforms the other compared schemes. For instance, when 100 nodes are considered, the accuracy of SM-ARP is 4% greater than the second best BSVR-ARP scheme.

The prediction of past attackers and integrated detection of the attackers in packet forwarding

process is the main reason for this significant improvement.

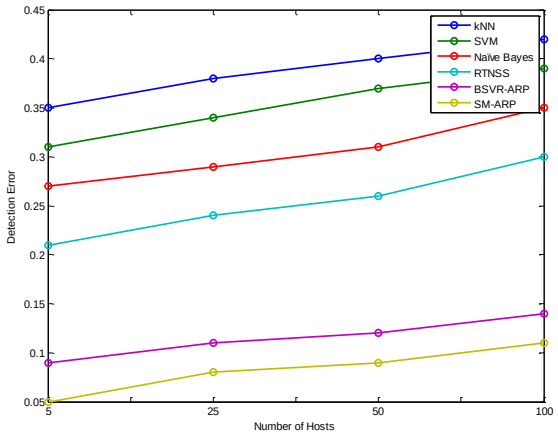


Fig.7. Detection error

Fig.7 shows the comparison of the ARP protection schemes based on the detection error. When the attackers are initiated at each case of host nodes, the traffic is automatically increased and leads to fluctuations in the detection schemes. The scheme that effectively handles this situation performs better than the other. The detection error of SM-ARP in these situations is very less than the other compared schemes at any number of host nodes. For 100 nodes, the detection error of SM-ARP is reduced by 6% than the second best BSVR-ARP scheme which is largely due to the highly accurate detection of the attacker host nodes.

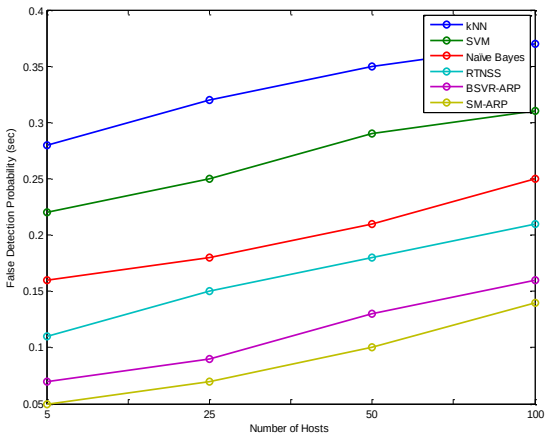


Fig.8. False detection probability

Fig.8 shows the false detection probability comparison of the ARP protection schemes. False detection probability of the proposed SM-ARP is very less than the other models due to the accurate detection of the attackers even when the false traffic packets generated by the attackers are high in number. Since this property of SM-ARP effectively tackles the attackers, in 100 node scenario, the false detection probability reduced by 3% than the second best BSVR-ARP scheme.

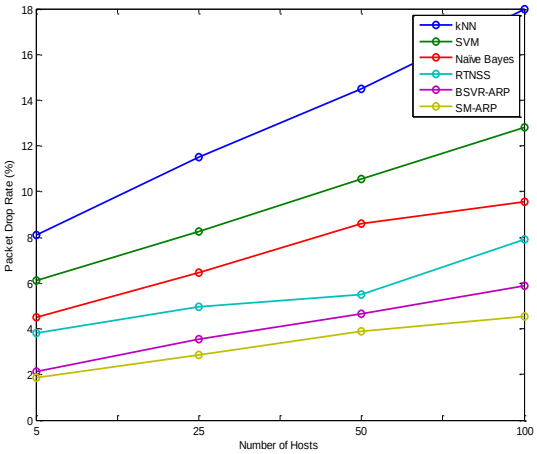


Fig.9. Packet drop rate

Fig.9 shows the packet drop rate comparison of the ARP protection schemes. When the number of host nodes increase, the network traffic increases and cause congestion of data packets. This scenario worsens when the attackers' starts sending forged ARP packets and also fake traffic packets to avoid detection from the protection units. Even in such cases, the SM-ARP scheme effectively tackles the attackers than the other schemes and decreases the forceful packet drop rate. The packet drop rate of SM-ARP very less than the other compared schemes at any number of host nodes. For example, when 100 host nodes are initiated, the packet drop rate of SM-ARP is reduced by 2% than the second best BSVR-ARP scheme. Thus from the evaluation results, it can be inferred that the proposed SM-ARP performs better than the other compared schemes for improved detection of ARP spoofing attacks.

V. CONCLUSION

The problem of ARP spoofing attacks through packet forwarding relay strategy has been considered in this paper and an effective protection scheme is developed using the Stochastic Markovian game model called SM-ARP. This scheme utilized the stationary Markov model to initiate the collision based complete information game model to structure the attacker in a legitimate network during packet forwarding. The two-player model illustrated in this article demonstrates the accurate detection of attacker hosts and provides solution for tackling them. The experiments are performed using an application for student marks management system to evaluate the performance of the proposed scheme. The results proved that the SM-ARP model improves the detection accuracyof ARP attacksby 4% with 5% less time and 6% less error than BSVR-ARP and also outperforms the other existing detection schemes. The empirical results have shown greater improvements of ARP spoofing detection using SM-ARP, but there is still room for improvements. The future research directions include the study and investigation of possibility of employing new attack strategies that would become higher risks in user networks. Also, it is intended to analyse the hybrid attack strategies of ARP spoofing and model the SM-ARP to be more adaptive to next level future attack strategies.

REFERENCES

1. A. M. Colman, “Game theory and experimental games: The study of strategic interaction,”Elsevier, 2013.
2. C. Divya and D. F. X. Christopher, “Security against ARP Spoofing Attacks using Bayesian Support Vector Regression,” International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8, no. 7, pp. 636-644, 2019.
3. D. Kukreja, S. K.Dhurandherand B. V. R. Reddy, “Power aware malicious nodes detection for securing MANETs against packet forwarding misbehavior attack,”Journal of Ambient Intelligence and Humanized Computing, vol. 9, no. 4, pp. 941-956, 2018.
4. D. Moon, J. D. Lee, Y. S. JeongandJ. H. Park, “RTNSS: a routing trace-based network security system for preventing ARP spoofing attacks,”The Journal of Supercomputing, vol. 72, no. 5, pp. 1740-1756, 2016.
5. F. Afghah, A. Razi, and A. Abedi, “Stochastic game theoretical model for packet forwarding in relay networks,”Telecommunication Systems, vol. 52, no. 4, pp. 1877-1893, 2013.
6. F. Ubaid, R. Amin, F. B. Ubaidand M. M.Iqbal, M. M. “Mitigating address spoofing attacks in hybrid SDN,”Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 4, pp. 562-570, 2017.
7. H. S. Kang, J. H.Sonand C. S. Hong, “Defense technique against spoofing attacks using reliable ARP table in cloud computing environment,” In 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), IEEE, pp. 592-595, 2015.
8. J. Singhand V.Grewal, “A survey of different strategies to pacify ARP poisoning attacks in wireless networks,”International Journal of Computer Applications, vol. 116, no. 11, 2015.
9. J. Xia, Z. Cai, G. Huand M.Xu, “An active defense solution for ARP spoofing in OpenFlow network,”Chinese Journal of Electronics, vol. 28, no. 1, pp. 172-178, 2019.
10. K. Matsufuji, S. Kobayashi, H. Esakiand H.Ochiai, “ARP Request Trend Fitting for Detecting Malicious Activity in LAN,” In International Conference on Ubiquitous Information Management and Communication, Springer, Cham, pp. 89-96, 2019.
11. M. Nourianand P. E.Caines, “ϵ-Nash mean field game theory for nonlinear stochastic dynamical systems with major and minor agents,"SIAM Journal on Control and Optimization, vol. 51, no. 4, pp. 3302-3331, 2013.
12. M. S. Song, J. D. Lee, Y. S.Jeong, H. Y.Jeongand J. H. Park, “DS-ARP: a new detection scheme for ARP spoofing attacks based on routing trace for ubiquitous environments,”The Scientific World Journal, vol. 2014, 2014.
13. N. R.Enciso, O. J. S.Parraand E.Upegui, “ARP Attack Detection Software Poisoning and Sniffers in WLAN Networks Implementing Supervised Machine Learning,” In International Conference on Mobile, Secure, and Programmable Networking, Springer, Cham, pp. 240-250, 2018.
14. O. S. Younes, “Securing ARP and DHCP for mitigating link layer attacks,”Sādhanā, vol. 42, no. 12, pp. 2041-2053, 2017.
15. R. P. Singh, N. Dhandaand K. K.Agrawal, “Evaluation of address resolution protocol and essential security issues,” In 2017 IEEE International Conference on Intelligent Sustainable Systems (ICISS)pp. 1088-1091, 2017.
16. R. Perlman, C. Kaufman, and M.Speciner, “Network security: private communication in a public world,”Pearson Education India, 2016.
17. S. HijaziandM. S. Obaidat, “Address resolution protocol spoofing attacks and security approaches: A survey,”Security and Privacy, vol. 1, no. 1, pp. e49, 2019.
18. S. Singh, D. Singh and A. M. Tripathi, “Two-Phase Validation Scheme for Detection and Prevention of ARP Cache Poisoning,” In Progress in Advanced Computing and Intelligent Engineering, Springer, Singapore, pp. 303-315, 2019.
19. S. U.Ullasand J. Sandeep, “Reliable Monitoring Security System to Prevent MAC Spoofing in Ubiquitous Wireless Network,” In Advances in Big Data and Cloud Computing, Springer, Singapore, pp. 141-153, 2019.
20. S. Venkatramuluand C. G. Rao, “Various solutions for address resolution protocol spoofing attacks,”International Journal of Scientific and Research Publications, vol. 3, no. 7, pp. 1, 2013.
21. S. Y. Nam, S. Djuraev andM. Park, “Collaborative approach to mitigating ARP poisoning-based Man-in-the-Middle attacks,”Computer Networks, vol. 57, no. 18, pp. 3866-3884, 2013.
22. Sudhakarand R. K.Aggarwal, “A Security Approach and Prevention Technique against ARP Poisoning,” In International Conference on Information and Communication Technology for Intelligent Systems, Springer, Cham, pp. 39-49, 2017.
23. Y. Kim, S. Ahn, N. C.Thang, D. Choiand M. Park, “ARP Poisoning Attack Detection Based on ARP Update State in Software-Defined Networks,” In 2019 IEEE International Conference on Information Networking (ICOIN), pp. 366-371, 2019.
24. Z. Sasanand M.Salehi, “SDN-based defending against ARP poisoning attack,”Journal of Advances in Computer Research, vol. 8, no. 2, pp. 95-102, 2017.
25. Z. Trabelsi andW. El-Hajj, “On investigating ARP spoofing security solutions,”International Journal of Internet Protocol Technology, vol. 5, no. 1, pp. 92, 2010.

BIOGRAPHY

Ms. C. Divya is currently pursuing Ph.D in Computer Science in Rathnavel Subramaniam College of Arts and Science, Coimbatore under Bharathiar University. She has obtained her M.Phil (Computer Science) in the area of Network Security and Cryptography from Bharathidasan University. Her research areas include Network Security and Cryptography. She has published paper in International Conferences and Journals.

Dr.D.Francis Xavier Christopher received his Ph.D., in the area of Networking from Bharathiar University, Coimbatore in 2014 from Bharathiar University, Coimbatore. He obtained his M.Phil, in the area of Networking from Bharathiar University, Coimbatore in 2002. At present he is working as a Director, School of Computer Studies in Rathnavel Subramaniam College of Arts and Science, Coimbatore. His research interest lies in the area of Networking and Software Engineering. He has published 27 research papers in various reputed journals ranking with international standard. He served as a key note speaker for various research conferences country wide.